State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
146	A	Nevada Card Access System (NCAS) Administration	05/01/2016	1 of 7

1.0 PURPOSE

To establish a standard for the data entry and personnel database management of the Nevada Card Access System (NCAS) Security Management Application.

2.0 SCOPE

This standard applies to all state agencies meeting the requirements identified in the State Information Security Consolidated Policy, Section 1.1, Scope and Applicability and who are attached to NCAS.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

The EITS NCAS administrator, state entity NCAS security administrator(s) have the responsibility to ensure compliance with this standard. The NCAS Security Administrators are responsible for disseminating this standard and implementation within their units.

5.0 RELATED DOCUMENTS

EITS Security Standard 101, Personnel Security Standard
EITS Security Standard 109, Physical Access Control and PIV Clearance Standard
EITS Security Form 111, PIV Card and Access Request Form
Software House training and user manuals
EITS NCAS user manuals

6.0 STANDARDS

6.0.1 GENERAL PROGRAMMING AND ADMINISTRATION

A. The Office of Information Security (OIS) is responsible for the creation and administration of all partitions operated by EITS/OIS.

B. Participating entities are responsible to assign a primary and back up administrator to administrate their partition. The back-up administrator should have privileges equal to the primary administrator to perform all functions within NCAS. In the absence of an assigned primary and back up administrator OIS can provide assistance.

C. Partitions not administered by EITS/OIS are the responsibility of the participating entity. Upon request OIS will provide assistance with the creation of security objects.

D. Upon request OIS will provide programming and On the Job Training (OJT) for all entities.

E. Programming privileges are assigned based on delegated authority and the principle of least privilege.

F. Security administrators have delegated authority to administrate all partitions.

G. Partition administrators are assigned to entities to administer security objects and personnel within their home partition.

H. Selected partition administrators are assigned to entities with more than one partition. Selected partition administrators have the same delegated authority as a partition administrator in multiple partitions. Selected partition administers administrate all security objects and personnel within the selected partitions they are assigned.

I. Partition coordinators are assigned by selected partitions administrators and partition administrators to manage personnel records and PIV card issuance. Partition coordinators cannot administrate security objects only personnel records and card issuance.

J. Partitioned Security objects in the NCAS application are security objects that can be viewed, edited, or deleted by selected partition administrators, or partition administrators within their home partition. Please see appendix “A” for list of partitioned security objects.

K. Non-partitioned security objects are objects that can be viewed, edited, or deleted by all partition security administrators system wide. Please see appendix “B” for a list of non-partitioned security objects.

L. Partition administrators shall not view, edit, or delete shared partitioned security objects outside of their home partition(s) without permission from the primary partition administrator responsible for the security objects.

6.0.2 PROGRAMMING STANDARDIZATION AND DATA INTEGRITY

A. Partition administrators programming the NCAS application are required to standardize all entries to maintain business continuity and data integrity.

B. Partition administrators shall identify all security objects within their entity partition through the use of a unique abbreviated identifier of their entity name.

Examples of acceptable abbreviated entity names:

1) Department of Public Safety = DPS
2) Enterprise IT Services = EITS
3) Secretary of State = SOS

C. Programming entries into NCAS that are unique to an entity and a specific division within that entity are required to be identified by an abbreviated entity name, abbreviated Division name, and an abbreviated city/region name (if applicable), where the security object exists. Each sub category requires a hyphen separating the Department, Division, and city/region.

Example of an acceptable naming convention:

1) Department of Public Safety = DPS
2) Division of Records and Technology = RT
3) Carson City = CC

D. Please see appendix Security objects that require abbreviated names to include Division, and city/region (if applicable).

6.0.3 PERSONNEL DATA ENTRY

A. Partition administrators are responsible for the input and auditing of all personnel records within their partition(s).

B. Each personnel record shall be assigned to an individual to maintain integrity and accountability of each personnel record. This best practice allows the State of Nevada to provide accurate auditing capabilities while protecting State buildings, property, and assets and assists in facilitating a safe environment for all building occupants.

C. All personnel records must contain the first name, last name, and person type. If a Personal Identity Verification card (PIV card) is issued the card must have an activation and expiration date. PIV cards should not be issued for a period of time greater than four years or the anticipated retirement date of an employee. Contractor PIV Cards should not be issued greater than the negotiated contract expiration date.

D. Physical access should be granted on the principle of least privilege. This best practice minimizes the unauthorized access to State buildings, property and assets.

E. The NCAS administrator is prohibited to grant access to any facility, property, or leased buildings without the written consent of the building partition administrator or entity head.

F. If an employee transfers to another department outside of your partition(s), and remains in state service contact the NCAS administrator and inform the administrator

of the transfer. The NCAS administrator will transfer the employee to the appropriate entity and contact the partition administrator of the receiving entity.

6.0.4 NCAS CHANGE CONTROL

A. Participating entities shall inform EITS/OIS of any changes to the Partition Administrator roles and responsibility within NCAS. Upon notice the NCAS administrator will add, edit, or delete partition administrator's privilege(s) as requested by the entity head.

B. NCAS administration is performed through the use of the NCAS administration and monitoring client applications. The clients connect to the NCAS server through entities local LAN and SilverNet. The NCAS server is a shared resource for authorized entities. This shared resource requires system maintenance and changes based on user requests and system/application updates. Planned outages shall be performed during a service window from 5:00AM-7:00AM daily. During this service window all administration and monitoring client applications should be closed.

C. Personnel record formats (i.e. drop down browser, tabs, and enumerated fields) requiring modification must be requested in writing (email acceptable) by the partition administrator. Modifications to personnel record formats can only be performed by a NCAS administrator. Modifications to personnel record formats require all administration client applications closed and exited from the NCAS server. Changes will be requested through the EITS helpdesk and be performed during the next available business day.

6.0.5 PARTITION ADMINISTRATORS

A. Each entity should have two partition administers with equal administration privileges appointed by the entity head.

B. An IntegraScan and finger print FBI background check must be performed on all personnel performing the duties of a partition administrator or selected partition administrator.

C. Partition administrators are responsible for the data administration and standardization of all security objects and personnel records.

D. Partition administrators are responsible for assigning NCAS administration and monitoring users within their partition(s).

E. Partition administrators are responsible for delegating authority to partition coordinators for the data input and issuance of PIV cards.

F. Partition administrators are responsible for all network connections, TCPIP connections, and entity hardware between NCAS equipment and SilverNet.

G. Partition administrators are responsible for the installation and updating of all NCAS desktop applications within their partitions.

7.0 DEFINITIONS/BACKGROUND

PERSONAL IDENTITY VERIFICATION CARD – PIV Card is an identification card with technology encoded or embedded into the cards design through the use of a micro chip, magnetic strip or proximity technology that is used to verify an individual's identification and access on multiple systems. A PIV card can be used as an identification card, physical access control card, and fuel card on state fueling sites and in the future used as a credential to log into IT systems and applications.

SECURITY ADMINISTRATOR – This level of administration allows users full access to all windows, menus, and tabs including default templates and allows the security administrators to edit user passwords. If the NCAS application is upgraded in the future, security administrator privilege will have full access to new windows automatically.

HOME PARTITION – A home partition is identified by the partition the personnel record is assigned to. All personnel are assigned to one partition and that is considered their "Home Partition".

PARTITION ADMINISTRATOR – This level of administration allows users to configure and maintain the common data in the NCAS database to include create, edit, delete, or view data in their home partition.

SELECTED PARTITION ADMINISTRATOR – This level of administration allows users to configure and maintain the common data in the NCAS database to include create, edit, delete, or view data in their selected partitions.

PARTITION COORDINATOR – This level of coordination allows users to selected windows and menus associated with personnel records and PIV card issuance.

SECURITY OBJECT – A security object is an object in the system other than a report or personnel record. Several examples of security objects include doors, inputs, clearances, and areas.

PARTITION –A partition in the NCAS System is a segment of the database that is divided into separate groups of security objects and personnel. Partition Administrators/Coordinators are typically assigned one partition known as their "home partition" where they can create and edit data. Security Administrators and Selected Partition administrators are assigned in one partition, but can administrate more than one partition.

8.0 EXCEPTIONS/OTHER ISSUES

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

APPENDIX

APPENDIX A

1) Personnel and personnel groups
2) Clearances
3) Time Specifications
4) Doors and door groups
5) Elevators and elevator groups
6) Nodes (includes activity printers)

Note: All other security objects are shared with all partition/selected partition administrators. Partition/selected partition administrators have delegated authority to change any non-partitioned security objects outside of their home partition. This administration privilege is a default delegated authority within the CCURE●9000 application by the manufacturer and cannot be changed.

APPENDIX B

a. Areas
b. Badge layouts
c. Events
d. Guard Tour
e. Holidays (view only)
f. Holiday lists (view only)
g. Keypad Commands
h. Maps
i. Recipients
10) All group except personnel/door groups
11) Time Zones (view only)
12) Advanced Process controls
13) Communication Ports
14) iSTAR Controllers
15) Host modems
16) NetVue (video tour & video view)
17) RM LCD messages
18) Reader Status Messages

APPENDIX C

a. Configurable Reports
b. Areas
c. Badge Layouts
d. Clearances
e. Doors
f. Events
g. Guard Tours
h. Intrusion zones
i. Keypad Command
10) Maps
11) Output
12) Reader
13) Nodes
14) Page Messages
15) Time Specifications
16) Group
17) APC's
18) Communication Ports
19) Host Modem
20) iSTAR Cluster
21) NetVue
22) Input
23) RM LCD Messages
24) Reader Status Messages

State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
146	A	Nevada Card Access System (NCAS) Administration	05/01/2016	7 of 7

Approved By		
Title	**Signature**	**Date**
State Information Security Committee	Approved by Committee	5/1/2016
State Chief Information Security Officer (CISO)	Signature on File	5/25/2016
State Chief Information Officer (CIO)	Signature on File	6/13/2016

Document History		
Revision	**Date**	**Change**
A	05/01/16	Initial Release – Formerly EITS Standard 112